UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/786,454	02/26/2004	Sarvar Patel	29250-002013/US	4912

7590 06/03/2011

HARNESS, DICKEY & PIERCE, P.L.C.
P.O. Box 8910
Reston, VA 20195

EXAMINER	
TOLENTINO, RODERICK	

ART UNIT	PAPER NUMBER
2439	

MAIL DATE	DELIVERY MODE
06/03/2011	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/786,454	**Applicant(s)** PATEL ET AL.	
	Examiner RODERICK TOLENTINO	**Art Unit** 2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03/21/2011*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 February 2004* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. Claims 1 – 24 are pending.

In view of the Appeal Bried filed on 03/21/2011, PROSECUTION IS HEREBY REOPENED. A new grounds of rejection as been set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below:

/Edan Orgad/

Supervisory Patent Examiner, Art Unit 2439.

Response to Arguments

2. Applicant's arguments with respect to claims 1 and 24 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claim 5 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

4. As per claim 5, limitation recites “wherein the second cryptosync changes between communications sessions” however, in claim 1 the second cryptosync lasts for multiple sessions thus saying that the cryptosync should not change between sessions. For purposes of examination it will be interpreted to be the second cryptosync has the ability of being changed or replaced.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and

> the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1, 4, 6, 7, 11 and 12 are are rejected under 35 U.S.C. 103(a) as being unpatentable over Meandzija et al. U.S. PG-Publication No. (2005/0086468) in view of Malcolm et al. U.S. PG-Publication No. (2004/0078334).

7. As per claims 1, Meandzija teaches the first cryptosync having a life limited to the communication session, the comnmnication session being defined as a period of time a channel for communication exists between the two communication devices (Meandzija, Paragraph 0073, session certificate which is only valid for a single session) but fails to teach deriving, at a network element, a value of a first cryptosync for the communication session based on a value of a second cryptosync and the second cryptosync having a life extending over multiple communication sessions. However, in an analogous art Malcolm teaches deriving, at a network element, a value of a first cryptosync for the communication session based on a value of a second cryptosync (Malcolm, Paragraph 0145, certificate derived from root certificate) and the second cryptosync having a life extending over multiple communication sessions (Malcolm, Paragraph 0145, certificate derived from root certificate, the root certificate is being interpreted to be the second cryptosync which will last over multiple sessions since all the signed certificates will stem from the root).

8. At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Malcolm's Information management system Meandzija's digital certificate related to the user terminal hardware in a wireless network because it

offers the advantage of ensuring that the transmission of data by their staff is always carried out securely (Malcolm, Paragraph 0028).

9. As per claim 4, Meandzija as modified teaches the second cryptosync is used for verifying message integrity by at least one of the two devices (Meandzija, Paragraph 0007, communications between user terminal and access points).

10. As per claim 6, Meandzija as modified teaches deriving step derives the first cryptosync as at least a portion of the second cryptosync (Malcolm, Paragraph 0145, certificate derived from root certificate).

11. As per claim 7, Meandzija as modified teaches the deriving step derives the first cryptosync as at least a portion of the second cryptosync and a fixed bit sequence (Malcolm, Paragraph 0145, certificate derived from root certificate).

12. As per claim 11, Meandzija as modified teaches the deriving step derives a portion of the first cryptosync as the second cryptosync (Malcolm, Paragraph 0145, certificate derived from root certificate).

13. As per claim 12, Meandzija as modified teaches the deriving step derives a first portion of the first cryptosync as the second cryptosync and derives a second portion of the first cryptosync as a fixed bit sequence (Malcolm, Paragraph 0145, certificate derived from root certificate).

14. Claims 2 and 3 are rejected under 35 U.S.C. 103(a) as being unpatentable over Meandzija et al. U.S. PG-Publication No. (2005/0086468) and Malcolm et al. U.S. PG-

Publication No. (2004/0078334) in view of Burch et al. U.S. PG-Publication No. (2005/0172116).

15. As per claim 2, Meandzija fails to teach the second cryptosync is used for message encryption by at least one of the two devices. However in an analogous art Burch teaches the second cryptosync is used for message encryption by at least one of the two devices (Burch, Paragraphs 0004 and 0023, certificate encrypts communications).

16. At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Burch's techniques for dynamically establishing and managing trust relationships with Meandzija's digital certificate related to the user terminal hardware in a wireless network because it offers the advantage of improving trust relationships (Burch, Paragraph 0008).

17. As per claim 3, Meandzija as modified teaches the second cryptosync is used for verifying message integrity by at least one of the two devices (Meandzija, Paragraph 0007, communications between user terminal and access points).

18. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over

19. Meandzija et al. U.S. PG-Publication No. (2005/0086468) in view of Malcolm et al. U.S. PG-Publication No. (2004/0078334) and Somin et al. U.S. PG-Publication No. (2005/0177715)

20. As per claim 5, Meandzija fails to teach the second cryptosync changes between communication sessions. However, in an analogous art Somin teaches the second cryptosync changes between communication sessions (Somin, Paragraph 0043, new root certificate needed).

21. At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Somin's system for managing identities with Meandzija's digital certificate related to the user terminal hardware in a wireless network because it offers the advantage of effectively resolve the communications issues of addressing, identity verification, and trust extension (Somin, Paragraph 0007).

22. Claims 8 – 10 and 13 – 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Meandzija et al. U.S. PG-Publication No. (2005/0086468) in view of Malcolm et al. U.S. PG-Publication No. (2004/0078334) in further view of Rezaiifar et al. U.S. Patent No. (6,980,658).

23. As per claim 8, Meandzija fails to teach the deriving step derives most significant bits of the first cryptosync as the portion of the second cryptosync and derives least significant bits of the first cryptosync as the fixed bit sequence. However, in an analogous art Rezaiifat teaches the deriving step derives most significant bits of the first cryptosync as the portion of the second cryptosync and derives least significant bits of the first cryptosync as the fixed bit sequence (Rezaiifar, Col. 4 Lines 46 – 62, bit sequence).

24. At the time the invention was made, it would have been obvious to a person of ordinary skill in the art, to use Rezaiifar's method and apparatus for encrypting transmissions in a communication system with Meandzija's digital certificate related to the user terminal hardware in a wireless network because it offers the advantage of maintaining encryption protocols to prevent the disclosure of communications between parties (Rezaiifar, Col. 1 Lines 66 – 67 and Col. 2 Lines 1 – 2).

25. As per claim 9, Meandzija as modified teaches the fixed bit sequence is a string of 0s (Rezaiifar, Col. 9 Lines 11 – 22, EID value of Zero).

26. As per claim 10, Meandzija as modified teaches the deriving step derives a 32 most significant bits of the first cryptosync as the second cryptosync and derives a 32 least significant bits of the first cryptosync as a string of 0s (Rezaiifar, Col. 9 Lines 11 – 22, EID value of Zero).

27. As per claim 13, Meandzija as modified teaches the fixed bit sequence is a string of 0s (Rezaiifar, Col. 9 Lines 11 – 22, EID value of Zero).

28. As per claim 14, Meandzija as modified teaches the deriving step comprises: performing a pseudo-random function on the second cryptosync; and generating the first cryptosync from output of the pseudo-random function (Rezaiifar, Col. 8 Lines 15 – 21, randomly chosen).

29. As per claim 15, Meandzija as modified teaches the generating step generates the first cryptosync as the output of the pseudo-random function (Rezaiifar, Col. 8 Lines 15 – 21, randomly chosen).

30. As per claim 16, Meandzija as modified teaches the deriving step is performed at a base station (Rezaiifar, Col. 3 Lines 36 – 45, mobile devices and base stations).

31. As per claim 17, Meandzija as modified teaches the deriving step is performed at a mobile station (Rezaiifar, Col. 3 Lines 36 – 45, mobile devices and base stations).

32. As per claim 18, Meandzija as modified teaches encrypting a frame of information to send from the at least one of the two devices using the first cryptosync (Rezaiifar, Col. 2 Lines 19 – 23, encryption).

33. As per claim 19, Meandzija as modified teaches the frame of information is a radio link protocol, RLP, frame (Rezaiifar, Col. 6 Lines 45 – 56, RLP frames).

34. As per claim 20, Meandzija as modified teaches incrementing the first cryptosync after the encrypting step (Rezaiifar, Col. 2 Lines 38 - 48, incrementing).

35. As per claim 21, Meandzija as modified teaches decrypting a frame of information received at the at least one of the two devices using the first cryptosync (Rezaiifar, Col. 5 Lines 56 – 67, decryption).

36. As per claim 22, Meandzija as modified teaches the frame of information is a radio link protocol, RLP, frame (Rezaiifar, Col. 6 Lines 45 – 56, RLP frames).

37. As per claim 23, Meandzija as modified teaches incrementing the first cryptosync after the decrypting step (Rezaiifar, Col. 2 Lines 38 – 48, incrementing).

38. Claim 24 is rejected under 35 U.S.C. 103(a) as being unpatentable over

39. Meandzija et al. U.S. PG-Publication No. (2005/0086468) in view of Malcolm et al. U.S. PG-Publication No. (2004/0078334) and Burch et al. U.S. PG-Publication No. (2005/0172116).

40. As per claim 24, Meandzija teaches the first cryptosync having a life limited to the communication session, the communication session being defined as a period of time a channel for communication exists between the two communication devices (Meandzija, Paragraph 0073, session certificate which is only valid for a single session) but fails to teach deriving, at a network element, a value of a first cryptosync for the communication session based on a value of a second cryptosync and the second cryptosync having a life extending over multiple communication sessions and [cryptosync] used to encrypt further communication between the two devices. However, in an analogous art Malcolm teaches deriving, at a network element, a value of a first cryptosync for the communication session based on a value of a second cryptosync (Malcolm, Paragraph 0145, certificate derived from root certificate) and the second cryptosync having a life extending over multiple communication sessions (Malcolm, Paragraph 0145, certificate derived from root certificate, the root certificate is being interpreted to be the second cryptosync which will last over multiple sessions since all the signed certificates will stem from the root) and Burch teaches [cryptosync] used to encrypt further communication between the two devices (Burch, Paragraphs 0004 and 0023, certificate encrypts communications).

41. At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Malcolm's Information management system Meandzija's

digital certificate related to the user terminal hardware in a wireless network because it offers the advantage of ensuring that the transmission of data by their staff is always carried out securely (Malcolm, Paragraph 0028).

42. At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Burch's techniques for dynamically establishing and managing trust relationships with Meandzija's digital certificate related to the user terminal hardware in a wireless network because it offers the advantage of improving trust relationships (Burch, Paragraph 0008).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to RODERICK TOLENTINO whose telephone number is (571)272-2661. The examiner can normally be reached on Monday - Friday 9am to 5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan Orgad can be reached on (571) 272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Roderick Tolentino
Examiner
Art Unit 2439

Roderick Tolentino
/R. T./
Examiner, Art Unit 2439

/Edan Orgad/
Supervisory Patent Examiner, Art Unit 2439